

Planned list of Activities And Validation Process For Execution of VAPT

STRYKER, INDIA



Planned list of Activities and Validation Process for Execution of VAPT

Warning: THIS DOCUMENT MAY CONTAIN INFORMATION THAT COULD SEVERELY DAMAGE OR IMPACT THE INTEGRITY AND SECURITY OF THE ORGANIZATION IF DISCLOSED PUBLICLY. THIS DOCUMENT SHOULD BE SAFEGUARDED AT ALL TIMES AND MAINTAINED IN A SECURE AREA WHEN NOT IN USE. G'SECURE LABS ASSUMES NO RESPONSIBILITY OR LIABILITY FOR THE SECURITY OF THIS DOCUMENT AFTER DELIVERY TO THE ORGANIZATION NAMED HEREIN. IT IS THE ORGANIZATION'S RESPONSIBILITY TO SAFEGUARD THIS MATERIAL AFTER DELIVERY.

THIS REPORT CONTAINS PROPRIETARY INFORMATION THAT IS NOT TO BE SHARED, COPIED, DISCLOSED OR OTHERWISE DIVULGED WITHOUT THE EXPRESS WRITTEN CONSENT OF G' SECURE LABS OR THEIR DESIGNATED REPRESENTATIVE. USE OF THIS REPORTING FORMAT BY OTHER THAN G' SECURE LABS OR ITS SUBSIDIARIES IS STRICTLY PROHIBITED AND MAY BE PROSECUTED TO THE FULLEST EXTENT OF THE LAW.

Disclaimer: THE RECOMMENDATIONS CONTAINED IN THIS REPORT ARE BASED ON INDUSTRY STANDARD "BEST PRACTICES". BEST PRACTICES ARE, BY NECESSITY, GENERIC IN NATURE AND MAY NOT TAKE INTO ACCOUNT EXACERBATING OR MITIGATING CIRCUMSTANCES. THESE RECOMMENDATIONS, EVEN IF CORRECTLY APPLIED, MAY CAUSE CONFLICTS IN THE OPERATING SYSTEM OR INSTALLED APPLICATIONS, ANY RECOMMENDED CHANGES TO THE OPERATING SYSTEM OR INSTALLED APPLICATION SHOULD FIRST BE EVALUATED IN A NON-PRODUCTION ENVIRONMENT BEFORE BEING DEPLOYED IN THE PRODUCTION ENVIRONMENT.

G' SECURE LABS



www.gsecurelabs.com

Recipient:

Name/role	Company
Deepak	Stryker

Document Version:

Na	me of the Author	Version	Title	Date
Arı	unesh Mishra	1.0	Planned list of Activities And Validation Process For Execution of VAPT	April 7th, 2022



www.gsecurelabs.com

Table of Contents

1.	Summary		 5
	•		
2.	Planned List of Activities and Validation Process	••••	 5







1. Summary

Stryker has assigned the task of carrying out vulnerability assessment and penetration testing of their SmartMedic Platform by G'Secure Labs team. This is planned list of activities and validation process for execution of VAPT task. The version 1.0 detailed planned list of activities described about each validation process task. The steps or protocols which has been shared in this file according to the particular Smart medic component mentioned in the specific row with respect to the vulnerabilities mapped to the components.

2. Planned List of Activities and Validation Process

Threat Event(s)	Vulnerabilities	Asset	Planned list of Activities And Validation Process For Execution of VAPT
Deliver undirected malware (CAPEC-185)	Unprotected external USB Port on the tablet/devices.	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Unprotected external USB Port on the tablet/devices.	Smart medic (Stryker device) System Component	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.







5 !:		6 1 12 (6: 1 1 1 1 1	14)6
Deliver	External communications and	Smart medic (Stryker device)	1) Create Android malware
undirected malware	communications and exposure for	System Component	2) Transfer the malware to
(CAPEC-185)	communciation		tablet/Smart Medic Device
(3 23 233)	channels from and to		3) Malware execution on the device
	application and devices like tablet and		4) Exploit the devices with respect to vulnerability
	smartmedic device.		5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information
			gathering.
			7) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities
			8) Exploit the found loopholes while
			VA scanning using kali tools.
Deliver	External	Tablet Resources - web cam,	1) Create Android malware
undirected	communications and	microphone, OTG devices,	2) Transfer the malware to
malware	exposure for	Removable USB, Tablet	tablet/Smart Medic Device
(CAPEC-185)	communciation channels from and to	Application, Network interfaces (Bluetooth, Wifi)	3) Malware execution on the device
	application and	(Bluetootii, Will)	4) Exploit the devices with respect to
	devices like tablet and		vulnerability
	smartmedic device.		5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information
			gathering.
			7) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities
			8) Exploit the found loopholes while
			VA scanning using kali tools.
Deliver undirected	Legacy system identification if any	Smart medic (Stryker device) System Component	1) Create Android malware
malware	identification if any	System component	2) Transfer the malware to
(CAPEC-185)			tablet/Smart Medic Device
			3) Malware execution on the device
			4) Exploit the devices with respect to vulnerability
			5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information
			gathering.
			7) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities
			8) Exploit the found loopholes while
			VA scanning using kali tools.
Deliver	Legacy system	Tablet Resources - web cam,	1) Create Android malware
undirected	identification if any	microphone, OTG devices,	2) Transfer the malware to





		Demonship JCD T-1-1	tablet/Coopert NA - di - D - : '
malware (CAPEC-185)		Removable USB, Tablet Application, Network interfaces	tablet/Smart Medic Device
(CAI EC-103)		(Bluetooth, Wifi)	3) Malware execution on the device
		, , , , , , , , , , , , , , , , , , , ,	4) Exploit the devices with respect to
			vulnerability
			5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information
			gathering.
			7) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities
			8) Exploit the found loopholes while
- "			VA scanning using kali tools.
Deliver undirected	Ineffective patch	Device Maintainence tool (Hardware/Software)	NA
malware	management of firware, OS and	(Hardware/Software)	
(CAPEC-185)	applications thoughout		
,	the information		
	system plan		
Deliver	Ineffective patch	Tablet Resources - web cam,	1) Create Android malware
undirected malware	management of	microphone, OTG devices,	2) Transfer the malware to
(CAPEC-185)	firware, OS and applications thoughout	Removable USB, Tablet Application, Network interfaces	tablet/Smart Medic Device
(CAI LC 105)	the information	(Bluetooth, Wifi)	3) Malware execution on the device
	system plan	(2.0.00000.,,	4) Exploit the devices with respect to
			vulnerability
			5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information
			gathering.
			7) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities
			8) Exploit the found loopholes while
			VA scanning using kali tools.
Deliver	Ineffective patch	Smart medic (Stryker device)	1) Create Android malware
undirected malware	management of firware, OS and	System Component	2) Transfer the malware to
(CAPEC-185)	applications thoughout		tablet/Smart Medic Device
(5. 1. 2. 2. 2. 7	the information		3) Malware execution on the device
	system plan		4) Exploit the devices with respect to
			vulnerability
			5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information
			gathering.
			7) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities







			8) Exploit the found loopholes while
Deliver undirected malware (CAPEC-185)	Lack of plan for periodic Software Vulnerability Management	Device Maintainence tool (Hardware/Software)	VA scanning using kali tools. NA
Deliver undirected malware (CAPEC-185)	Lack of plan for periodic Software Vulnerability Management	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Lack of plan for periodic Software Vulnerability Management	Smart medic (Stryker device) System Component	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver undirected malware (CAPEC-185)	Unprotected network port(s) on network devices and connection points	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning







			for the distant to
			for the identifying unknown
			vulnerabilities
			8) Exploit the found loopholes while
- II			VA scanning using kali tools.
Deliver undirected	Unprotected network	Smart medic (Stryker device)	1) Create Android malware
malware	port(s) on network devices and	System Component	2) Transfer the malware to
(CAPEC-185)	connection points		tablet/Smart Medic Device
(1 1 1 1)			3) Malware execution on the device
			4) Exploit the devices with respect to vulnerability
			5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information
			gathering.
			7) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities
			8) Exploit the found loopholes while
			VA scanning using kali tools.
Deliver	Unencrypted data at	Tablet Resources - web cam,	1) Create Android malware
undirected malware	rest in all possible locations	microphone, OTG devices, Removable USB, Tablet	2) Transfer the malware to
(CAPEC-185)	locations	Application, Network interfaces	tablet/Smart Medic Device
(6/11/20/105)		(Bluetooth, Wifi)	3) Malware execution on the device
			4) Exploit the devices with respect to vulnerability
			5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information
			gathering.
			7) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities
			8) Exploit the found loopholes while
			VA scanning using kali tools.
			9) Use sniffing tool to sniff the data
			at motion and MITM
Deliver	Unencrypted data in	Smart medic (Stryker device)	1) Create Android malware
undirected malware	flight in all flowchannels	System Component	2) Transfer the malware to
(CAPEC-185)	Howchalliels		tablet/Smart Medic Device
(5 25 255)			3) Malware execution on the device
			4) Exploit the devices with respect to
			vulnerability 5) Check for the open ports
			5) Check for the open ports
			6) Exploit the open ports found while assessment and information
			gathering.
			7) Vulnerability Assessment scanning





			1
			for the identifying unknown vulnerabilities
			8) Exploit the found loopholes while
			VA scanning using kali tools.
Deliver	Unencrypted data in	Tablet Resources - web cam,	1) Create Android malware
undirected malware	flight in all flowchannels	microphone, OTG devices, Removable USB, Tablet	2) Transfer the malware to
(CAPEC-185)	nowchanners	Application, Network interfaces	tablet/Smart Medic Device
(0 20 200)		(Bluetooth, Wifi)	3) Malware execution on the device
			4) Exploit the devices with respect to vulnerability
			5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information
			gathering.
			7) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities
			8) Exploit the found loopholes while
			VA scanning using kali tools.
Deliver	Outdated -	Device Maintainence tool	NA
undirected malware	Software/Hardware	(Hardware/Software)	
(CAPEC-185)			
Deliver	Outdated -	Smart medic (Stryker device)	1) Create Android malware
undirected	Software/Hardware	System Component	2) Transfer the malware to
malware			tablet/Smart Medic Device
(CAPEC-185)			3) Malware execution on the device
			4) Exploit the devices with respect to
			vulnerability
			5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information
			gathering.
			7) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities
			8) Exploit the found loopholes while
D. I.		711.10	VA scanning using kali tools.
Deliver undirected	Outdated -	Tablet Resources - web cam,	1) Create Android malware
malware	Software/Hardware	microphone, OTG devices, Removable USB, Tablet	2) Transfer the malware to
(CAPEC-185)		Application, Network interfaces	tablet/Smart Medic Device
,		(Bluetooth, Wifi)	3) Malware execution on the device
			4) Exploit the devices with respect to
			vulnerability 5) Chack for the open parts
			5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information







Deliver directed malware (CAPEC-185)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Device Maintainence tool (Hardware/Software)	gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. NA
Deliver directed malware (CAPEC-185)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Smart medic (Stryker device) System Component	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	Unprotected external USB Port on the tablet/devices.	Wireless Network device	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to





			1
			vulnerability
			5) Check for the open ports
			6) Use sniffing tool to sniff the data
			at motion and MITM
			7) Exploit the open ports found while
			assessment and information
			gathering.
			8) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilit <mark>ies</mark>
			9) Exploit the found loopholes while
			VA scanning using kali tools.
Deliver directed	Unprotected external	Tablet Resources - web cam,	1) Create Android malware
malware	USB Port on the	microphone, OTG devices,	2) Transfer the malware to
(CAPEC-185)	tablet/devices.	Removable USB, Tablet	tablet/Smart Medic Device
		Application, Network interfaces (Bluetooth, Wifi)	3) Malware execution on the device
		(Bidetootii, Will)	4) Exploit the devices with respect to
			vulnerability
			5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information
			gathering.
			7) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities
			8) Exploit the found loopholes while
			VA scanning using kali tools.
Deliver directed	Unprotected external	Smart medic app (Stryker Azure	1) Vulnerability Assessment scanning
malware	USB Port on the	Cloud Web Application)	for the identifying unknown
(CAPEC-185)	tablet/devices.		vulnerabilities of web application.
			2) Check for the open ports using
			nmap, other kali tools
			3) Exploit the found loopholes while
			VA Scanning using the Burpsuite, kali
			tools.
			4) Exploit the open ports using kali
			tools.
Deliver directed	External	Tablet Resources - web cam,	1) Create Android malware
malware	communications and	microphone, OTG devices,	2) Transfer the malware to
(CAPEC-185)	exposure for	Removable USB, Tablet	tablet/Smart Medic Device
	communciation	Application, Network interfaces	3) Malware execution on the device
	channels from and to	(Bluetooth, Wifi)	4) Exploit the devices with respect to
	application and		vulnerability
	devices like tablet and		5) Check for the open ports
	smartmedic device.		6) Exploit the open ports found while
			assessment and information
			gathering.





Deliver directed malware (CAPEC-185)	Ineffective patch management of firware, OS and applications thoughout the information	Device Maintainence tool (Hardware/Software)	7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. NA
Deliver directed malware (CAPEC-185)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Smart medic (Stryker device) System Component	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Deliver directed malware (CAPEC-185)	Unprotected network port(s) on network devices and connection points	Smart medic (Stryker device) System Component	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability







			5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information
			gathering.
			7) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities
			8) Exploit the found loopholes while
			VA scanning using kali tools.
Deliver directed	Unprotected network	Tablet Resources - web cam,	1) Create Android malware
malware	port(s) on network	microphone, OTG devices,	2) Transfer the malware to
(CAPEC-185)	devices and	Removable USB, Tablet	tablet/Smart Medic Device
	connection points	Application, Network interfaces	3) Malware execution on the device
		(Bluetooth, Wifi)	4) Exploit the devices with respect to
			vulnerability
			5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information
			gathering.
			7) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities
			8) Exploit the found loopholes while
			VA scanning using kali tools.
Deliver directed	Unprotected network	Wireless Network device	1) Create Android malware
malware	port(s) on network		2) Transfer the malware to
(CAPEC-185)	devices and		tablet/Smart Medic Device
	connection points		3) Malware execution on the device
			4) Exploit the devices with respect to
			vulnerability
			5) Check for the open ports
			6) Use sniffing tool to sniff the data
			at motion and MITM
			7) Exploit the open ports found while
			assessment and information
			gathering.
			8) Vulnerability Assessment scanning for the identifying unknown
			vulnerabilities
			9) Exploit the found loopholes while
Doliver directed	InCoguro Configuration	Smart modic and (Straker Association	VA scanning using kali tools.
Deliver directed malware	InSecure Configuration for Software/OS on	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning
(CAPEC-185)	Mobile Devices,	Cloud Web Application)	for the identifying unknown
(5/ 11 23 105)	Laptops, Workstations,		vulnerabilities of web application.
	and Servers		2) Check for the open ports using
			nmap, other kali tools
			3) Exploit the found loopholes while





			VA C
			VA Scanning using the Burpsuite, kali tools.
			4) Exploit the open ports using kali
			tools.
Deliver directed	InSecure Configuration	Tablet Pessurees, web sam	1) Create Android malware
malware	for Software/OS on	Tablet Resources - web cam, microphone, OTG devices,	'
(CAPEC-185)	Mobile Devices,	Removable USB, Tablet	2) Transfer the malware to
(1 1 1 1)	Laptops, Workstations,	Application, Network interfaces	tablet/Smart Medic Device
	and Servers	(Bluetooth, Wifi)	3) Malware execution on the device
			4) Exploit the devices with respect to vulnerability
			5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information
			gathering.
			7) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities
			8) Exploit the found loopholes while
			VA scanning using kali tools.
Deliver directed	Unencrypted data at	Tablet Resources - web cam,	1) Create Android malware
malware	rest in all possible	microphone, OTG devices,	2) Transfer the malware to
(CAPEC-185)	locations	Removable USB, Tablet	tablet/Smart Medic Device
		Application, Network interfaces	3) Malware execution on the device
		(Bluetooth, Wifi)	4) Exploit the devices with respect to
			vulnerability
			5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information
			gathering.
			7) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities
			8) Exploit the found loopholes while
			VA scanning using kali tools.
			9) Use sniffing tool to sniff the data
			at motion and MITM
Deliver directed	Unencrypted data at	Tablet OS/network details &	1) Create Android malware
malware	rest in all possible	Tablet Application	2) Transfer the malware to
(CAPEC-185)	locations		tablet/Smart Medic Device
			3) Malware execution on the device
			4) Exploit the devices with respect to
			vulnerability
			5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information
			gathering.
			7) Vulnerability Assessment scanning







			for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. 9) Use sniffing tool to sniff the data
Deliver directed malware (CAPEC-185)	Unencrypted data at rest in all possible locations	Smart medic app (Stryker Azure Cloud Web Application)	at motion and MITM 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Use sniffing tool to sniff the data at motion and MITM
Gaining Access ([S]TRID[E])	Unprotected network port(s) on network devices and connection points	Tablet OS/network details & Tablet Application	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Gaining Access ([S]TRID[E])	Unprotected network port(s) on network devices and connection points	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Unprotected network port(s) on network devices and connection points	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device







		Application, Network interfaces (Bluetooth, Wifi)	4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Gaining Access ([S]TRID[E])	Devices with default passwords needs to be checked for bruteforce attacks	Authenication/Authorisation data	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Gaining Access ([S]TRID[E])	Devices with default passwords needs to be checked for bruteforce attacks	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Devices with default passwords needs to be checked for bruteforce attacks	Interface/API Communication	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools.







			4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Authenication/Authorisation data	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Gaining Access ([S]TRID[E])	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Checking authentication modes for possible hacks and bypasses	Authenication/Authorisation data	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali







			tools. 4) Exploit the open ports using kali tools.
			5) Brute Force attempt for the authentication/authorization on the open port
			6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Gaining Access ([S]TRID[E])	Checking authentication modes for possible hacks and bypasses	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Checking authentication modes for possible hacks and bypasses	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Controlled Use of Administrative Privileges over the network	Authenication/Authorisation data	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port





Gaining Access ([S]TRID[E])	Controlled Use of Administrative Privileges over the network	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Unprotected external USB Port on the tablet/devices.	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Maintaining Access (TTP)	Devices with default passwords needs to be checked for bruteforce attacks	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Maintaining Access (TTP)	Devices with default passwords needs to be checked for bruteforce attacks	Smart medic app (Azure Portal Administrator)	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.







Maintaining Access (TTP)	Devices with default passwords needs to be checked for bruteforce attacks	Authenication/Authorisation data	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Maintaining Access (TTP)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Maintaining Access (TTP)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Maintaining Access (TTP)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Authenication/Authorisation data	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.





			5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Maintaining Access (TTP)	Checking authentication modes for possible hacks and bypasses	Smart medic app (Stryker Azure Cloud Web Application)	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Maintaining Access (TTP)	Checking authentication modes for possible hacks and bypasses	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Maintaining Access (TTP)	Controlled Use of Administrative Privileges over the network	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Maintaining Access (TTP)	Controlled Use of Administrative Privileges over the network	Authenication/Authorisation data	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.





			E) Bruto Force attempt for the
			5) Brute Force attempt for the authentication/authorization on the
			open port
			6) Exploit related to Brute Force
			attempt for the
			authentication/authorization on the
			open port
Clearing Track	InSecure Configuration	Tablet Resources - web cam,	1) Create Android malware
(TTP)	for Software/OS on Mobile Devices,	microphone, OTG devices, Removable USB, Tablet	2) Transfer the malware to
	Laptops, Workstations,	Application, Network interfaces	tablet/Smart Medic Device
	and Servers	(Bluetooth, Wifi)	3) Malware execution on the device
		,	4) Exploit the devices with respect to
			vulnerability
			5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information
			gathering.
			7) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities
			8) Exploit the found loopholes while
			VA scanning using kali tools.
Clearing Track	InSecure Configuration	Smart medic app (Stryker Azure	1) Vulnerability Assessment scanning
(TTP)	for Software/OS on	Cloud Web Application)	for the identifying unknown
	Mobile Devices,		vulnerabilities of web application.
	Laptops, Workstations,		2) Check for the open ports using
	and Servers		nmap, other kali tools
			3) Exploit the found loopholes while
			VA Scanning using the Burpsuite, kali
			tools.
			4) Exploit the open ports using kali
			tools.
Clearing Track	Outdated -	Tablet Resources - web cam,	1) Create Android malware
(TTP)	Software/Hardware	microphone, OTG devices,	2) Transfer the malware to
		Removable USB, Tablet	tablet/Smart Medic Device
		Application, Network interfaces	3) Malware execution on the device
		(Bluetooth, Wifi)	4) Exploit the devices with respect to
			vulnerability
			5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information
			gathering.
			7) Vulnerability Assessment scanning
			for the identifying unknown vulnerabilities
			8) Exploit the found loopholes while
			VA scanning using kali tools.





a		T.11.18	Ta\c + A + + + +
Clearing Track (TTP)	Lack of configuration controls for IT assets in the informaion system plan	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Clearing Track (TTP)	Lack of configuration controls for IT assets in the informaion system plan	Device Maintainence tool (Hardware/Software)	NA
Clearing Track (TTP)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Clearing Track (TTP)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Device Maintainence tool (Hardware/Software)	NA
Clearing Track (TTP)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Tablet OS/network details & Tablet Application	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability







			5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Clearing Track (TTP)	The static connection digaram between devices and applications with provision for periodic updation as per changes	Device Maintainence tool (Hardware/Software)	NA
Clearing Track (TTP)	The static connection digaram between devices and applications with provision for periodic updation as per changes	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Elevation of privilege (STRID[E])	Controlled Use of Administrative Privileges over the network	Authenication/Authorisation data	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the







			authentication/authorization on the
			open port
Elevation of	Controlled Use of	Smart medic app (Azure Portal	1) Vulnerability Assessment scanning
privilege	Administrative	Administrator)	for the identifying unknown
(STRID[E])	Privileges over the	,	vulnerabilities of web application.
	network		2) Check for the open ports using
			nmap, other kali tools
			3) Exploit the found loopholes while
			VA Scanning using the Burpsuite, kali
			tools.
			4) Exploit the open ports using kali
			tools.
Denial of service	Unprotected network	Wireless Network device	1) Create Android malware
(STRI(D)E)	port(s) on network		2) Transfer the malware to
	devices and		tablet/Smart Medic Device
	connection points		3) Malware execution on the device
			4) Exploit the devices with respect to
			vulnerability
			5) Check for the open ports
			6) Use sniffing tool to sniff the data
			at motion and MITM
			7) Exploit the open ports found while
			assessment and information
			gathering.
			8) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities
			9) Exploit the found loopholes while
			VA scanning using kali tools.
Denial of service	Unprotected network	Tablet OS/network details &	1) Create Android malware
(STRI(D)E)	port(s) on network	Tablet Application	2) Transfer the malware to
	devices and		tablet/Smart Medic Device
	connection points		3) Malware execution on the device
			4) Exploit the devices with respect to
			vulnerability
			5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information
			gathering.
			7) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities
			8) Exploit the found loopholes while
			VA scanning using kali tools.
Information	Unencrypted data at	Data at Rest	1) Vulnerability Assessment scanning
disclosure	rest in all possible		for the identifying unknown
(STR(I)DE)	locations		vulnerabilities of web application.





			2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM 8) Use sniffing tool to sniff the data at motion and MITM
Information disclosure (STR(I)DE)	Unencrypted data in flight in all flowchannels	Data in Motion	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Information disclosure (STR(I)DE)	Weak Encryption Implementaion in data at rest and in motion tactical and design wise	Data at Rest	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.





			5) Brute Force attempt for the
			authentication/authorization on the
			open port
			6) Exploit related to Brute Force
			attempt for the
			authentication/authorization on the
			open port
			7) Use sniffing tool to sniff the data
			at motion and MITM
Information	Weak Encryption	Data in Motion	1) Vulnerability Assessment scanning
disclosure (STR(I)DE)	Implementaion in data at rest and in motion		for the identifying unknown
(STR(I)DE)	tactical and design		vulnerabilities of web application.
	wise		2) Check for the open ports using
			nmap, other kali tools
			3) Exploit the found loopholes while
			VA Scanning using the Burpsuite, kali tools.
			4) Exploit the open ports using kali
			tools.
			5) Brute Force attempt for the
			authentication/authorization on the
			open port
			6) Exploit related to Brute Force
			attempt for the
			authentication/authorization on the
			open port
			7) Use sniffing tool to sniff the data
			at motion and MITM
Information	Weak Algorthim	Data at Rest	1) Vulnerability Assessment scanning
disclosure	implementation with		for the identifying unknown
(STR(I)DE)	respect cipher key size		vulnerabilities of web application.
			2) Check for the open ports using
			nmap, other kali tools
			3) Exploit the found loopholes while
			VA Scanning using the Burpsuite, kali
			tools.
			4) Exploit the open ports using kali tools.
			5) Brute Force attempt for the
			authentication/authorization on the
			open port
			6) Exploit related to Brute Force
			attempt for the
			authentication/authorization on the
			open port
			7) Use sniffing tool to sniff the data
			at motion and MITM





Infanc-+!-	Mank Al	Data in Matin	4) \/la analailite A
Information disclosure (STR(I)DE)	Weak Algorthim implementation with respect cipher key size	Data in Motion	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Information disclosure (STR(I)DE)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Information disclosure (STR(I)DE)	Unencrypted Network segment throught the information flow	Data in Motion	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port





			T
			 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data
			at motion and MITM
Information disclosure (STR(I)DE)	Insecure communications in networks (hospital)	Data in Motion	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Data Access (STR[I]DE)	Unprotected network port(s) on network devices and connection points	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Data Access (STR[I]DE)	Unprotected network port(s) on network devices and connection points	Wireless Network device	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports





			C) 11: (f(:+1)
			6) Use sniffing tool to sniff the data
			at motion and MITM
			7) Exploit the open ports found while
			assessment and information
			gathering.
			8) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities
			9) Exploit the found loopholes while
			VA scanning using kali tools.
Data Access	Unprotected network	Tablet OS/network details &	1) Create Andr <mark>oid</mark> malware
(STR[I]DE)	port(s) on network	Tablet Application	2) Transfer the malware to
	devices and connection points		tablet/Smart Medic Device
	connection points		3) Malware execution on the device
			4) Exploit the devices with respect to
			vulnerability
			5) Check for the open ports
			6) Exploit the open ports found while
			assessment and information
			gathering.
			7) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities
			8) Exploit the found loopholes while
			VA scanning using kali tools.
Data Access	Devices with default	Data at Rest	1) Vulnerability Assessment scanning
(STR[I]DE)	passwords needs to be		for the identifying unknown
	checked for bruteforce attacks		vulnerabilities of web application.
	attacks		2) Check for the open ports using
			nmap, other kali tools
			3) Exploit the found loopholes while
			VA Scanning using the Burpsuite, kali
			tools.
			4) Exploit the open ports using kali
			tools.
			5) Brute Force attempt for the
			authentication/authorization on the
			open port
			6) Exploit related to Brute Force
			attempt for the
			authentication/authorization on the
			open port
			7) Use sniffing tool to sniff the data
			at motion and MITM
Data Access	Devices with default	Authenication/Authorisation	1) Vulnerability Assessment scanning
(STR[I]DE)	passwords needs to be	data	for the identifying unknown
			vulnerabilities of web application.





	checked for bruteforce attacks		2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Data Access (STR[I]DE)	Devices with default passwords needs to be checked for bruteforce attacks	Data in Motion	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Data Access (STR[I]DE)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Data at Rest	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force





			attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Data Access (STR[I]DE)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Azure Portal Administrator)	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Data Access (STR[I]DE)	Controlled Use of Administrative Privileges over the network	Smart medic app (Azure Portal Administrator)	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Data Access (STR[I]DE)	Unprotected external USB Port on the tablet/devices.	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Open network port exploit (TTP)	Unprotected network port(s) on network devices and connection points	Tablet OS/network details & Tablet Application	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports





			 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Open network port exploit (TTP)	Unprotected network port(s) on network devices and connection points	Wireless Network device	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Use sniffing tool to sniff the data at motion and MITM 7) Exploit the open ports found while assessment and information gathering. 8) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 9) Exploit the found loopholes while VA scanning using kali tools.
Open network port exploit (TTP)	Unencrypted Network segment throught the information flow	Tablet OS/network details & Tablet Application	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools.
Open network port exploit (TTP)	Unencrypted Network segment throught the information flow	Wireless Network device	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports





			6) Use sniffing tool to sniff the data
			at motion and MITM
			7) Exploit the open ports found while
			assessment and information
			gathering.
			8) Vulnerability Assessment scanning
			for the identifying unknown
			vulnerabilities
			9) Exploit the found loopholes while
			VA scanning using kali tools.
Open network	Controlled Use of	Smart medic app (Azure Portal	1) Vulnerability Assessment scanning
port exploit	Administrative	Administrator)	for the identifying unknown
(TTP)	Privileges over the		vulnerabilities of web application.
	network		2) Check for the open ports using
			nmap, other kali tools
			3) Exploit the found loopholes while
			VA Scanning using the Burpsuite, kali
			tools.
			4) Exploit the open ports using kali
			tools.
Open network	Unencrypted data in	Data in Motion	1) Vulnerability Assessment scanning
port exploit	flight in all		for the identifying unknown
(TTP)	flowchannels		vulnerabilities of web application.
			2) Check for the open ports using
			nmap, other kali tools
			3) Exploit the found loopholes while
			VA Scanning using the Burpsuite, kali
			tools.
			4) Exploit the open ports using kali
			tools.
			5) Brute Force attempt for the
			authentication/authorization on the
			open port
			6) Exploit related to Brute Force
			attempt for the
			authentication/authorization on the
			·
			open port 7) Use sniffing tool to sniff the data
			at motion and MITM
Open network	Insecure	Tablet OS/network details &	1) Create Android malware
Open network port exploit	Insecure communications in	Tablet Application	'
(TTP)	networks (hospital)		2) Transfer the malware to
,	(tablet/Smart Medic Device
			3) Malware execution on the device
			4) Exploit the devices with respect to
			vulnerability
			5) Check for the open ports
			6) Exploit the open ports found while





Brute-force Attack (CAPEC-112)	Devices with default passwords needs to be checked for bruteforce attacks	Smart medic app (Stryker Azure Cloud Web Application)	assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	Devices with default passwords needs to be checked for bruteforce attacks	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	Devices with default passwords needs to be checked for bruteforce attacks	Azure Cloud DataBase	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Brute-force Attack (CAPEC-112)	The password complexity or location vulnerability. Like	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application.





			2) ()
	weak passwords and hardcoded passwords.		 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Azure Cloud DataBase	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Brute-force Attack (CAPEC-112)	Checking authentication modes for possible hacks and bypasses	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	Checking authentication modes	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application.





	for possible hacks and bypasses		 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	Weak Encryption Implementaion in data at rest and in motion tactical and design wise	Data at Rest	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM
Brute-force Attack (CAPEC-112)	Weak Encryption Implementaion in data at rest and in motion tactical and design wise	Data in Motion	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM







C:-I	1-C	Consist on a diagram (C)	4) Volumentility As
Social Engineering (TTP)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Smart medic app (Stryker Azure Cloud Web Application)	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Social Engineering (TTP)	Legacy system identification if any	Smart medic app (Stryker Azure Cloud Web Application)	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Social Engineering (TTP)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Social Engineering (TTP)	Checking authentication modes for possible hacks and bypasses	Interface/API Communication	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Social Engineering (TTP)	Checking authentication modes for possible hacks and bypasses	Smart medic app (Stryker Azure Cloud Web Application)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali





			Apple
			tools.
			4) Exploit the open ports using kali
Social Engineering (TTP)	Checking authentication modes for possible hacks and bypasses	Azure Cloud DataBase	tools. 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the
Social Engineering (TTP)	Checking authentication modes for possible hacks and bypasses	Smart medic app (Azure Portal Administrator)	open port 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Lack of evidence to conclude any malicious attempt/attack (ST[R]IDE)	Insufficient Logging information	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Lack of evidence to conclude any malicious attempt/attack (ST[R]IDE)	Insufficient Access permissions for accessing and modifying Log files	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali





			tools. 4) Exploit the open ports using kali tools.
Unauthorized Alterations (S[T]RIDE)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Azure Cloud DataBase	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Unauthorized Alterations (S[T]RIDE)	Insufficient Access permissions for accessing and modifying Log files	Azure Cloud DataBase	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Gaining Access ([S]TRID[E])	Error Info containing sensitive data for Failed Authentication attempts	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.





Gaining Access	Error Info containing	Azure Cloud DataBase	1) Vulnerability Assessment scanning
([S]TRID[E])	sensitive data for Failed Authentication attempts	Azure Ciouu Database	for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Gaining Access ([S]TRID[E])	Absence of additional security factor along with user identification	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Gaining Access ([S]TRID[E])	Absence of additional security factor along with user identification	Azure Cloud DataBase	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port
Gaining Access ([S]TRID[E])	Having no limit on the login attempts	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application.





			2) Check for the open ports using
			nmap, other kali tools
			3) Exploit the found loopholes while
			VA Scanning using the Burpsuite, kali
			tools.
			4) Exploit the open ports using kali
			tools.
Gaining Access	Having no limit on the	Azure Cloud DataBase	1) Vulnerability Assessment scanning
([S]TRID[E])	login attempts		for the identifying unknown
			vulnerabilities of web application.
			2) Check for the open ports using
			nmap, other kali tools
			3) Exploit the found loopholes while
			VA Scanning using the Burpsuite, kali
			tools.
			4) Exploit the open ports using kali
			tools.
			5) Brute Force attempt for the
			authentication/authorization on the
			open port
			6) Exploit related to Brute Force
			attempt for the
			authentication/authorization on the
			open port
Brute-force	Error Info containing	Smart medic app (Azure Portal	1) Vulnerability Assessment scanning
Attack (CAPEC-112)	sensitive data for Failed Authentication	Administrator)	for the identifying unknown
(CAPEC-112)	attempts		vulnerabilities of web application.
	attempts		2) Check for the open ports using
			nmap, other kali tools
			3) Exploit the found loopholes while
			VA Scanning using the Burpsuite, kali
			tools.
			4) Exploit the open ports using kali
			tools.
Brute-force	Error Info containing	Azure Cloud DataBase	1) Vulnerability Assessment scanning
Attack	sensitive data for		for the identifying unknown
(CAPEC-112)	Failed Authentication		vulnerabilities of web application.
	attempts		2) Check for the open ports using
			nmap, other kali tools
			3) Exploit the found loopholes while
			VA Scanning using the Burpsuite, kali
			tools.
			4) Exploit the open ports using kali
			tools.
			5) Brute Force attempt for the
			authentication/authorization on the
			open port





Brute-force Attack (CAPEC-112)	Absence of additional security factor along with user identification	Smart medic app (Azure Portal Administrator)	6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	Absence of additional security factor along with user identification	Azure Cloud DataBase	 Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. Check for the open ports using nmap, other kali tools Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. Exploit the open ports using kali tools. Brute Force attempt for the authentication/authorization on the open port Exploit related to Brute Force attempt for the authentication/authorization on the open port
Brute-force Attack (CAPEC-112)	Having no limit on the login attempts	Smart medic app (Azure Portal Administrator)	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.
Brute-force Attack (CAPEC-112)	Having no limit on the login attempts	Azure Cloud DataBase	 1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while





	VA Scanning using the Burpsuite, kali
	tools.
	4) Exploit the open ports using kali
	tools.
	5) Brute Force attempt for the
	authentication/authorization on the
	open port
	6) Exploit related to Brute Force
	attempt for the
	authentication/authorization on the
	open port







THE NETHERLAND

Maria Montessorilaan 3, 2719 DB Zoetermeer, The Netherlands

INDIA

B/81, Corporate House, Judges Bungalow Road, Bodakdev, Ahmedabad - 380054. India

www.gsecurelabs.com

Confidentiality Clause:

This document and any files with it are for the sole use of the intended recipient(s) and may contain confidential and privileged information. If you are not the intended recipient, please destroy all copies of the document. Any unauthorized review, use, disclosure, dissemination, forwarding, printing or copying of this document or any action taken in reliance on this document is strictly prohibited and may be unlawful. Copyright © Gateway Group